GOVERNMENT (AND ITS EXPENSIVE CONTRACTORS) REALLY NEED TO SECURE THEIR DATA COLLECTIONS

Given two recent high profile hacks, the government needs to either do a better job of securing its data collection and sharing process, or presume people will get hurt because of it.

After the hackers Crackas With Attitude hacked John Brennan, they went onto hack FBI's Deputy Director Mark Giuliano as well as a law enforcement portal run by the FBI. The hack of the latter hasn't gotten as much attention — thus far, WikiLeaks has not claimed to have the data, but upon closer examination of the data obtained, it appears it might provide clues and contact information about people working undercover for the FBI.

Then, the hackers showed Wired's Kim Zetter what the portal they had accessed included. Here's a partial list:

> Enterprise File Transfer Service—a web interface to securely share and transmit files.
>
> Cyber Shield Alliance—an FBI Cybersecurity partnership initiative "developed by Law Enforcement for Law Enforcement to proactively defend and counter cyber threats against LE networks and critical technologies," the portal reads. "The FBI stewards an array of cybersecurity resources and intelligence, much of which is now accessible to LEA's through the Cyber Shield Alliance."
>
> IC3—"a vehicle to receive, develop, and

> refer criminal complaints regarding the rapidly expanding arena of cyber crime."
>
> Intelink—a "secure portal for integrated intelligence dissemination and collaboration efforts"
>
> National Gang Intelligence Center—a "multi-agency effort that integrates gang information from local, state, and federal law enforcement entities to serve as a centralized intelligence resource for gang information and analytical support."
>
> RISSNET—which provides "timely access to a variety of law enforcement sensitive, officer safety, and public safety resources"
>
> Malware Investigator—an automated tool that "analyzes suspected malware samples and quickly returns technical information about the samples to its users so they can understand the samples' functionality."
>
> eGuardian—a "system that allows Law Enforcement, Law Enforcement support and force protection personnel the ability to report, track and share threats, events and suspicious activities with a potential nexus to terrorism, cyber or other criminal activity."

While the hackers haven't said whether they've gotten into these information sharing sites, they clearly got as far as the portal to the tools that let investigators share information on large networked investigations, targeting things like gangs, other organized crime, terrorists, and hackers. If hackers were to access those information sharing networks, they might be able to both monitor investigations into such networked crime groups, but also (using credentials they already hacked) to make false entries. And all that's before CISA will vastly expand this info sharing.

Meanwhile, the Intercept reported receiving 2.5 years of recorded phone calls — amounting to 70 million recorded calls — from one of the nation's largest jail phone providers, Securus. Its report focuses on proving that Securus is not defeat-listing calls to attorneys, meaning it has breached attorney-client privilege. As Scott Greenfield notes, that's horrible but not at all surprising.

But on top of that, the Intercept's source reportedly obtained these recorded calls by hacking Securus. While we don't have details of how that happened, that does mean all those calls were accessible to be stolen. If Intercept's civil liberties-motivated hacker can obtain the calls, so can a hacker employed by organized crime.

The Intercept notes that even calls to prosecutors were online (which might include discussions from informants). But it would seem just calls to friends and associates would prove of interest to certain criminal organizations, especially if they could pinpoint the calls (which is, after all, the point). As Greenfield notes, defendants don't usually listen to their lawyers' warnings — or those of the signs by the phones saying all calls will be recorded — and so they say stupid stuff to everyone.

> So we tell our clients that they cannot talk about anything on the phone. We tell our clients, "all calls are recorded, including this one." So don't say anything on the phone that you don't want your prosecutor to hear.
>
> Some listen to our advice. Most don't. They just can't stop themselves from talking. And if it's not about talking to us, it's about talking to their spouses, their friends, their co-conspirators. And they say the most remarkable things, in the sense of "remarkable" meaning "really damaging." Lawyers only know the stupid stuff they say to us. We learn the stupid stuff

> they say to others at trial. Fun times.

Again, such calls might be of acute interest to rival gangs (for example) or co-conspirators who have figured out someone has flipped.

It’s bad enough the government left OPM’s databases insecure, and with it sensitive data on 21 million clearance holders.

But it looks like key law enforcement data collections are not much more secure.